

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-117820

(P2001-117820A)

(43)公開日 平成13年4月27日(2001.4.27)

(51)Int.Cl.⁷

G 0 6 F 12/14

識別記号

3 1 0

F I

G 0 6 F 12/14

テ-マ-コード*(参考)

3 1 0 Z 5 B 0 1 7

審査請求 未請求 請求項の数15 OL (全 29 頁)

(21)出願番号 特願平11-293544

(22)出願日 平成11年10月15日(1999. 10. 15)

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72)発明者 黒田 康嗣

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 吉岡 孝司

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74)代理人 100074099

弁理士 大曾 義之 (外1名)

最終頁に続く

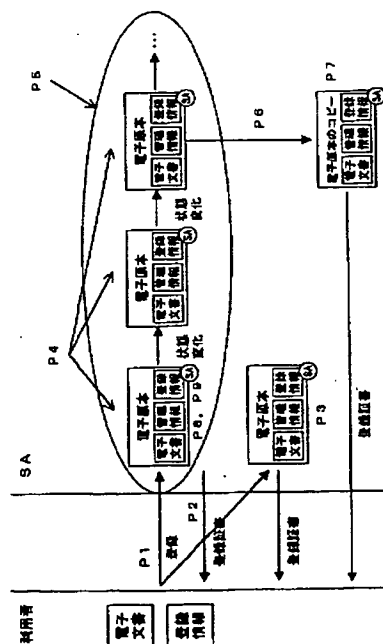
(54)【発明の名称】 電子原本管理装置および方法

(57)【要約】

【課題】 電子化された重要文書の原本をより安全に管理することが課題である。

【解決手段】 利用者のコンピュータ環境とは別に電子原本管理装置を設けて、電子文書を電子原本として登録する。電子原本管理装置は、電子原本を一意に識別するための登録証書を発行し、利用者は、発行された登録証書を用いて電子原本にアクセスする。

電子原本モデルを示す図



【特許請求の範囲】

【請求項 1】 電子情報を原本情報として登録する登録手段と、

前記電子情報に対して、該電子情報を論理的に一意に識別する論理識別情報と、該電子情報の物理的所在を表す所在識別情報とを付与する付与手段と、

前記論理識別情報と前記所在識別情報の組合せに基づく組合せ識別情報を用いて、前記原本情報を管理する管理手段と、

前記組合せ識別情報を含み、前記原本情報へのアクセスのために用いられる登録証書情報を発行する発行手段とを備えることを特徴とする電子原本管理装置。

【請求項 2】 利用者は、前記登録証書情報に含まれる前記組合せ識別情報を用いて、前記電子原本管理装置に登録された前記原本情報にアクセスすることを特徴とする請求項 1 記載の電子原本管理装置。

【請求項 3】 前記管理手段は、前記所在識別情報と前記電子情報が保存されている物理的所在とを比較し、該所在識別情報が該物理的所在に対応していなければ、該電子情報は不正コピーであると判断することを特徴とする請求項 1 記載の電子原本管理装置。

【請求項 4】 前記電子原本管理装置の識別情報、装置内の電子情報識別情報、オリジナルとコピーを識別するためのタイプ属性情報、およびタイムスタンプ情報から前記論理識別情報を作成する作成手段をさらに備え、前記管理手段は、該電子原本管理装置の識別情報と電子情報識別情報の組合せを原本系列識別情報として管理することを特徴とする請求項 1 記載の電子原本管理装置。

【請求項 5】 前記管理手段は、登録される電子情報をすべて原本情報として扱い、登録時には、オリジナルを表すタイプ属性情報を該登録される電子情報に付与することを特徴とする請求項 4 記載の電子原本管理装置。

【請求項 6】 前記電子情報のコピーの作成時には、前記管理手段は、前記原本系列識別情報と前記タイムスタンプ情報を変更せず、前記タイプ属性情報をコピーを表すタイプ属性情報に変更した論理識別情報を生成し、生成された論理識別情報を該電子情報のコピーに付与することを特徴とする請求項 5 記載の電子原本管理装置。

【請求項 7】 利用者は、前記登録証書情報に含まれる前記タイプ属性情報を参照することで、前記電子情報がオリジナルであるかコピーであるかを判断することを特徴とする請求項 4 記載の電子原本管理装置。

【請求項 8】 前記電子情報がコピーであるとき、前記利用者は、前記登録証書情報に含まれる前記タイムスタンプ情報を参照することで、該コピーがどの時点の電子情報のコピーであるかを判断することを特徴とする請求項 7 記載の電子原本管理装置。

【請求項 9】 前記原本情報の更新時には、前記管理手段は、前記原本系列識別情報と前記タイプ属性情報を変更せず、前記タイムスタンプ情報を変更して、更新前と

更新後の原本情報を管理することを特徴とする請求項 4 記載の電子原本管理装置。

【請求項 10】 前記管理手段は、前記原本情報の時系列な変化に応じて原本情報の一連のインスタンスを生成し、該一連のインスタンスを 1 つの原本系列として扱うことを特徴とする請求項 4 記載の電子原本管理装置。

【請求項 11】 前記電子原本管理装置に他の電子原本管理装置から原本情報が移動してきたとき、前記管理手段は、移動してきた原本情報の原本系列識別情報とタイプ属性情報を変更せず、タイムスタンプ情報を変更して、該移動してきた原本情報を管理することを特徴とする請求項 4 記載の電子原本管理装置。

【請求項 12】 電子情報の時系列な変化に応じて、対応する原本情報の一連のインスタンスを生成し、該一連のインスタンスを 1 つの原本系列として管理する管理手段と、

前記原本系列に対して原本系列識別情報を付与する付与手段と、

前記原本系列識別情報を含み、前記一連のインスタンスのうちの 1 つのインスタンスへのアクセスのために用いられる登録証書情報を発行する発行手段とを備えることを特徴とする電子原本管理装置。

【請求項 13】 電子情報を論理的に一意に識別する論理識別情報と該電子情報の物理的所在を表す所在識別情報との組合せに基づく組合せ識別情報を含む登録証書情報を格納する格納手段と、

前記登録証書情報を用いて、原本情報として登録された前記電子情報へのアクセスを要求する要求手段とを備えることを特徴とする電子原本アクセス装置。

【請求項 14】 電子情報を原本情報として登録し、前記電子情報に対して、該電子情報を論理的に一意に識別する論理識別情報と、該電子情報の物理的所在を表す所在識別情報とを付与し、

前記論理識別情報と前記所在識別情報の組合せに基づく組合せ識別情報を用いて、前記原本情報を管理し、前記組合せ識別情報を含む登録証書情報を用いて、前記原本情報にアクセスすることを特徴とする電子原本管理方法。

【請求項 15】 電子情報の時系列な変化に応じて、対応する原本情報の一連のインスタンスを生成し、前記一連のインスタンスを 1 つの原本系列として管理し、

前記原本系列に対して原本系列識別情報を付与し、前記原本系列識別情報を含む登録証書情報を用いて、前記一連のインスタンスのうちの 1 つのインスタンスにアクセスすることを特徴とする電子原本管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、文書の電子化に係り、電子化された重要文書の原本を管理する装置および

方法に関する。

【0002】

【従来の技術】従来、重要文書の原本は紙媒体として管理され、それらは、ファイリングして整理したりして管理されてきた。しかし、近年のパーソナルコンピュータの普及とネットワーク環境の拡大により、企業間取引や電子決済等の様々なサービスの電子化が進展し、紙媒体として扱われてきた重要文書が電子媒体に記録されて処理されている。電子化が進むにつれて、データベースと連携した文書管理アプリケーションが出現し、現在、それらのアプリケーションを用いて文書が管理されつつある。

【0003】

【発明が解決しようとする課題】しかしながら、従来の文書管理アプリケーションには、以下のような問題がある。

1. 利用者の管理下のコンピュータで文書が管理されるため、文書の作成日時等を容易に偽れる。
2. 利用者の管理下のコンピュータで文書が管理されるため、文書を容易に削除可能である。
3. 利用者の管理下のコンピュータで文書が管理されるため、文書を容易に改ざん可能である。たとえ、文書管理アプリケーションが文書操作の履歴を記録していたとしても、その履歴をも容易に改ざんすることができる。
4. 文書をコピーすると、全く同じ内容の電子文書ができてしまうため、どちらが本物の原本であるかわからなくなる。

【0004】このように、電子化文書には紙媒体にない様々な問題があるため、重要文書の電子化においては、運用面での制限が紙媒体以上に課せられている。このため、せっかく電子処理されるにもかかわらず、最終的には文書を紙媒体に出力して、契約や発注の処理を行ったり、法廷文書として保管しているのが現状である。

【0005】本発明の課題は、電子化された重要文書の原本をより安全に管理する装置および方法を提供することである。

【0006】

【課題を解決するための手段】図1は、本発明の電子原本管理装置の原理図である。図1の電子原本管理装置は、登録手段1、付与手段2、管理手段3、および発行手段4を備える。

【0007】本発明の第1の局面において、登録手段1は、電子情報を原本情報として登録し、付与手段2は、その電子情報に対して、電子情報を論理的に一意に識別する論理識別情報と、電子情報の物理的所在を表す所在識別情報とを付与する。管理手段3は、論理識別情報と所在識別情報の組合せに基づく組合せ識別情報を用いて、原本情報を管理し、発行手段4は、その組合せ識別情報を含み、原本情報へのアクセスのために用いられる登録証書情報を発行する。

【0008】登録手段1が登録する電子情報は、例えば、電子化された重要文書に対応し、登録された電子情報は、登録手段1内に保存される。また、電子情報の物理的所在は、例えば、登録手段1内で電子情報が保存されている場所（アドレス等）に対応する。管理手段3は、付与手段2により付与された論理識別情報と所在識別情報を組み合わせて組合せ識別情報を生成し、その組合せ識別情報を原本情報に付与する。そして、発行手段4は、その組合せ識別情報を含む登録証書情報を生成し、登録者等に発行する。

【0009】電子情報を原本情報として登録し、付与手段2は、その電子情報に対して、電子情報を論理的に一意に識別する論理識別情報と、電子情報の物理的所在を表す所在識別情報とを付与する。管理手段3は、論理識別情報と所在識別情報の組合せに基づく組合せ識別情報を用いて、原本情報を管理し、発行手段4は、その組合せ識別情報を含み、原本情報へのアクセスのために用いられる登録証書情報を発行する。

【0010】このような電子原本管理装置によれば、電子情報は登録されてはじめて原本情報として扱われるため、登録者側で生成された電子情報のコピーは原本情報ではないことを明確にすることができる。また、登録者および他の利用者は、発行された登録証書情報を用いて原本情報にアクセスするので、登録された原本情報を一意に識別することができる。したがって、原本管理の安全性が向上する。

【0011】また、本発明の第2の局面において、管理手段3は、電子情報の時系列な変化に応じて、対応する原本情報の一連のインスタンスを生成し、その一連のインスタンスを1つの原本系列として管理する。付与手段2は、原本系列に対して原本系列識別情報を付与し、発行手段4は、その原本系列識別情報を含み、一連のインスタンスのうちの1つのインスタンスへのアクセスのために用いられる登録証書情報を発行する。

【0012】原本情報のインスタンスは、登録された電子情報が更新等により変化した場合に生成され、管理手段3は、付与手段2により付与された原本系列識別情報を用いて、一連のインスタンスを管理する。そして、発行手段4は、その原本系列識別情報を含む登録証書情報を生成し、登録者等に発行する。

【0013】このような電子原本管理装置によれば、更新等により刻々と生成される電子情報の系列を1つのグループとして扱うことができる。また、登録者および他の利用者は、発行された登録証書情報を用いて各インスタンスにアクセスするので、登録された原本系列を一意に識別することができる。したがって、原本管理の安全性が向上する。

【0014】例えば、図1の登録手段1は、後述する図4の原本系列管理部34と文書保管部36に対応し、図1の付与手段2は、図4の物理ID作成部37と識別I

D作成部40に対応し、図1の管理手段3は、図4の原本系列管理部34に対応し、図1の発行手段4は、図4の原本系列管理部34と登録証書作成部35に対応する。

【0015】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態を詳細に説明する。本発明においては、利用者にサービスを提供するコンピュータ環境とは別に、電子原本管理装置を設ける。また、電子原本管理装置に登録される電子文書は、アプリケーションに依存した“原本”、“謄本”等の属性にかかわらず、すべて電子原本として扱われ、その電子原本に対して登録証書が発行される。すべて電子原本として扱うということは、電子文書を紙に出力した状態に対応し、以後、電子原本の利用者は、発行された登録証書を用いて電子原本にアクセスする。例えば、電子原本としては、次のようなものが登録される。

1. 有価証券、健康保険証、紙幣等。原本を提示することによって権利や価値を示したり、原本の譲渡を行うことができる。
2. 領収書等のように、商業活動で生成される文書（法廷文書）。原本を保管しておき、監査時等に証拠として提出することができる。
3. 戸籍謄本、登記簿謄本等のように、契約書に添付される文書。戸籍謄本や登記簿謄本は、戸籍や登記簿の原本に登録されている内容と同じであることを保証し、契約時には、身元を保証する原本として契約書とともに保管される。
4. 契約書等。同じ内容の契約書の原本を2部作成し、個々の原本を契約を交わした各当事者が保管する。
5. 遺言書、契約書等。弁護士や公証人役場等の第三者をたてて、原本を第三者が保管し、その謄本を当事者たちが保管する。
6. 議事録、企画書等のように、一般業務で生成される文書。これらの文書の原本を保管しておき、複数の当事者により共有する。
7. 官公庁や地方自治体で生成される文書。保管機関や公開レベルを設定して管理する。
8. 研究ノートや設計書等のように、特許紛争の際に証拠として提出される文書。
9. 電子顕微鏡で撮ったDNA（deoxyribonucleic acid）の写真や、風洞実験の様子を写したフィルム等のように、研究の証拠となる画像情報。

【0016】図2は、本実施形態において電子原本管理装置に保管される電子原本モデルを示している。図2において、セキュアアーカイバ（Secure Archiver, SA）は、電子原本管理装置に対応し、以下のような処理を行う。

P1：利用者側のコンピュータで処理され作成された電子文書は、SAに登録されてはじめて電子原本となる。

このように、電子文書をSAに登録してはじめて原本として扱うことで、利用者側で電子文書のコピーが行われて全く同じ電子文書が作成されても、それらは原本ではなく、SA内の電子文書が原本であることを明確にすることができる。

P2：次に、SAは、登録された電子文書（電子原本）に対して、登録証書を発行する。このように、SAが登録証書を発行し、利用者が登録証書を用いてSA内の電子原本にアクセスすることで、SA内の電子原本を一意に識別することが可能となる。

P3：次に、利用者側の同じ内容の電子文書をSAに二重登録しても、SA内では別々の原本として扱う。このように、SAに登録される電子文書を別々の電子原本として扱うことで、紙媒体では同じ内容を印刷しても物理的に別々の物として扱うことが可能であったように、たとえ同じ内容であったとしても、電子的に各々独立した原本であると識別することが可能となる。

P4：次に、ある電子原本に対して更新が行われた際には、各時点の電子文書をその原本のインスタンスとして保持する。また、各々のインスタンスに対して、登録証書を発行する。このように処理することで、利用者は登録証書を用いて、ある原本のある時点のインスタンスを取り出すことが可能となる。

P5：P4で保持された一連のインスタンスを1つの原本として扱う。このように処理することで、更新等で状態が変化する原本を1つの原本として扱うことが可能となる。

P6：次に、SAに登録されている電子原本からのコピーのみを電子原本のコピーとして扱う。このように処理することで、利用者側で発生するコピー文書と電子原本のコピーを明確に区別することが可能となる。

P7：次に、電子原本のオリジナルから作成されるコピーがどの時点の電子原本のコピーであるかを明確に区別する処理を行う。また、その電子原本のコピーに対して、登録証書を発行する。このように、どの時点の電子原本のコピーであるかを明確に示した登録証書を発行することで、利用者は、電子原本のコピーがどの時点のコピーであるかを明確に識別することが可能となる。

P8：次に、原本や謄本の属性等のアプリケーションから指定される登録情報と、コピーやオリジナル等の属性や作成日時等のSAが独自に管理する管理情報を電子文書と一体化して扱う。このように、アプリケーションとは独立して、電子文書、管理情報、および登録情報を一体化することで、たとえ文書が移動しても、移動先でその電子原本の属性を参照することが可能となる。

P9：次に、電子文書、管理情報、登録情報を一体化した形で改ざん検出情報（円で囲まれたSAにより表される部分）を作成する。このように、電子文書のみでなく、管理情報と登録情報を含めて改ざん検出情報を作成することで、電子文書、管理情報、および登録情報の

整合性が保持される。

【0017】図3は、上述したセキュアアーカイバを含む電子原本管理システムの構成図である。図3のシステムは、SA11、サービスクライアント（利用者端末）12、およびローカルな環境13を含み、サービスクライアント12とSA11の間と、2つのSA11間において、電子原本14がやり取りされる。文書レコード15は、図2の登録証書に対応し、SA11内の電子原本14へアクセスするために用いられる。

【0018】サービスクライアント12とSA11は、通信ネットワークに接続されており、サービスクライアント12は、電子原本登録時にSA11から発行される文書レコード15を用いて、SA11内の電子原本14にアクセスする。また、SA11間のやり取りにおいては、ネットワーク接続の場合は、サービスクライアント12とSA11の間の通信と同様に、文書レコード15を用いて電子原本14がやり取りされる。オフラインの場合は、セキュア媒体16を用いて電子原本14がやり取りされる。

【0019】サービスクライアント側のローカルな環境13は、会社内の1つの部署や事務所等で電子原本の唯一性等の安全性（原本性）を保証するシステムであり、ローカルSA21と利用者端末22を含む。ローカルSA21内に管理されている電子原本は、ローカルな環境13内のみで原本性が保証されており、他のSA11内の電子原本とはリンクしていない。ローカルSA21と外部のSA11の間では、通信ネットワークまたはセキュア媒体16を介して、電子原本の情報をやり取りすることができる。

【0020】図4は、図3のSA11の構成図である。図4のSA11は、ネットワークインタフェース31、要求解釈部32、返答作成部33、原本系列管理部34、登録証書作成部35、文書保管部36、物理ID作成部37、暗号処理部38、鍵保持部39、識別ID作成部40、時刻生成部41、装置ID保持部42、およびインクリメンタルカウンタ43を備える。

【0021】このうち、文書保管部36と物理ID作成部37は、ファイルシステムを構成し、暗号処理部38、鍵保持部39、識別ID作成部40、時刻生成部41、装置ID保持部42、およびインクリメンタルカウンタ43は、セキュリティハードウェアとして実装される。

【0022】図5は、SA11が行う処理のフローチャートである。SA11の1つのトランザクションは、クライアント12からの要求受信、要求に応じた装置内での処理、およびクライアント12への返答送信からなる。まず、ネットワークインタフェース31は、クライアント12からの要求を受信し（ステップST1）、要求解釈部32は、要求の種類を識別する（ステップST2）。

【0023】次に、原本系列管理部34は、各要求に従った処理を行い（ステップST3）、処理結果を作成する（ステップST4）。そして、返答作成部33は、クライアント12への返答メッセージを作成し（ステップST5）、ネットワークインタフェース31は、クライアント12へ返答メッセージを送信する（ステップST6）。これにより、1つのトランザクションが終了する。

【0024】例えば、クライアント12から文書の登録要求がくると、要求解釈部32は、要求の種類が文書登録であると解釈し、クライアント12から送付されてきた文書を原本系列管理部34に渡す。

【0025】次に、原本系列管理部34は、暗号処理部38を介して、識別ID作成部40に論理識別IDの作成を依頼し、文書保管部36に文書を格納する。識別ID作成部40は、時刻生成部41からタイムスタンプを取得し、装置ID保持部42からSA11の装置IDを取得し、インクリメンタルカウンタ43から装置内の文書IDを表すカウンタ値を取得して、論理識別IDを生成する。

【0026】また、暗号処理部38は、鍵保持部39に保持されている装置鍵（SAの個別鍵）を用いて、論理識別IDにデジタル署名を施し、原本系列管理部34に論理識別IDを渡す。また、物理ID作成部37は、文書の物理的な所在を表す物理IDを作成し、文書保管部36を介して原本系列管理部34に渡す。

【0027】原本系列管理部34は、論理識別IDと物理IDを連結して暗号処理部38に渡す。暗号処理部38は、鍵保持部39に保持されている装置鍵を用いて署名処理を行い、生成されたデジタルデータを識別IDとして原本系列管理部34に返す。原本系列管理部34は、受け取った識別IDを登録依頼された文書の識別情報として管理する。

【0028】次に、原本系列管理部34は、登録証書作成部35に文書レコードの作成を指示し、登録証書作成部35は、文書レコードを作成して原本系列管理部34に返す。そして、原本系列管理部34は、文書レコードを返答作成部33に渡し、返答作成部33は、クライアント12への返答メッセージを作成し、ネットワークインタフェース31を介してクライアント12に送付して、処理を終了する。図3のSA21の構成についても同様である。

【0029】次に、図6から図26までを参照しながら、図3のシステムが行う処理をより詳細に説明する。上述したように、SAは、電子原本の登録時に、登録証書として文書レコードを利用者に発行する。利用者は、文書レコードを用いてSA内の電子原本にアクセスしたり、原本の共有者に文書レコードを送付したりする。共有者は、送付されてきた文書レコードを用いてSAにアクセスすることによって、原本を利用することができ

る。文書レコードの要件は、以下の通りである。

1. 電子原本登録の事実を証明する。
2. SA内のどの原本に対して発行されたかを示す情報を提供する。
3. 利用者のどの電子文書が原本として登録されたかを示す情報を提供する。
4. 原本登録者（所有者）の情報を提供する。
5. アクセスすべきSAの情報を提供する。
6. 文書レコードの改ざんを検出する。

【0030】これらの要件から、SAは、図6に示すような情報を文書レコードの中に埋め込んで発行する。電子原本のハッシュ値41は、SAに登録されている原本の内容をハッシュ関数により圧縮して得られた値である。このハッシュ値41を利用者が持つ電子文書のハッシュ値と比較することによって、その電子文書が確かにSAに登録されている文書であることを確認することができる。したがって、ハッシュ値41は、登録の事実を証明する情報として用いられる。ハッシュ値41の代わりに、原本の内容を他の一方向性関数で変換した結果を用いてもよい。

【0031】識別ID42は、SA内の電子原本を一意に識別するための識別情報であり、論理識別IDと物理IDから生成される。SAは、文書レコードがどの電子原本に対して発行されたのかを示す情報として、識別IDを文書レコードに付加する。

【0032】利用者側の電子文書名53は、利用者側で管理しているファイル名に対応し、SA内の電子原本と利用者の電子文書に対応付ける情報として付加される。また、利用者ID54は、原本登録時の認証に用いられる識別情報であり、原本の登録者（所有者）の情報として文書レコードに付加される。

【0033】SAの接続先情報55は、SAのIP（Internet Protocol）アドレスやFQDN（Fully Qualified Domain Name）等に対応し、アクセスすべきSAの識別情報として文書レコードに付加される。また、SAの署名56は、文書レコードの発行時に、文書レコードの情報に対してSAが計算して添付する署名情報であり、文書レコードをSAが発行したことを示すお墨付き情報でもある。利用者は、署名56が添付された文書レコードをSAに送信し、電子文書の改ざんの有無を検証することができる。

【0034】次に、原本系列の管理について説明する。SAに登録された原本は、更新、移動、削除等の操作によりその状態が変化していく。SAは、状態が変化するたびに、その時点の原本のインスタンスを保持し、一連のインスタンスを原本系列として管理する。そして、その原本系列に原本系列IDを与えて、一意に識別する。これにより、サービスクライアントから見れば、その系列を1つの原本として特定し、取り出すことが可能となる。

【0035】図7は、原本系列IDにより原本系列を一意に識別する様子を示している。電子文書D1が電子文書D1-1としてSAに登録されると、SAは、電子文書D1-1に原本系列IDとしてSID1を与え、原本系列S1として管理する。

【0036】その後、電子文書D1に修正等が行われて原本の状態が変化し、再登録が行われると、SAは、SID1を原本系列IDとする電子文書D1-2のインスタンスを生成し、それを保持する。以後、状態変化が起こるたびに、電子文書D1-3、D1-4、D1-5のようなインスタンスが保持されていき、一連のインスタンスをSID1により識別する。

【0037】また、電子文書D1とは別に登録された電子文書D2には、新たに原本系列IDとしてSID2が与えられる。そして、電子文書D2の一連のインスタンスD2-1、D2-2、D2-3、D2-4、D2-5等は、SID2により識別され、原本系列S2として管理される。このとき、電子文書D2の内容が電子文書D1の内容とまったく同じでも、SAは、各々を別の電子原本として管理する。

【0038】このような原本系列IDを用いれば、状態変化によって生成される一連のインスタンスを1つの原本として識別することが可能である。しかし、法廷文書の監査等を行う場合には、ある原本系列の中の任意の時点のインスタンスを特定して、取り出す必要がある。そのため、SAは、原本系列の各時点のインスタンスにタイムスタンプを与える。

【0039】図8は、ある原本系列の中で、時系列に変化するインスタンスをタイムスタンプによって管理している様子を示している。電子文書D1が電子文書D1-1として登録されると、登録時点のタイムスタンプT1が与えられ、以後、状態変化のたびに、各インスタンスにタイムスタンプT2、T3、T4、T5等が与えられる。利用者は、原本系列IDとタイムスタンプを指定することにより、電子原本の任意の時点のインスタンスを特定して、取り出すことが可能となる。

【0040】次に、電子原本のオリジナルとコピーの管理の要件を明確にするために、まず、電子文書のコピーの問題を明確にする。電子文書をコピーすると、オリジナルとまったく同じ電子文書が存在することになるため、コピーが氾濫し、どれが本物の原本であるか識別不可能となる。このため、従来は、媒体にラベルを貼る等の運用方法によりコピーが管理されていた。

【0041】また、電子文書が不正にコピーされても、コピー元では、コピーされたことを識別することは不可能であり、また、コピー先では、コピーをオリジナルな電子文書として扱うことが可能となっている。なお、紙媒体の場合は、その質感からオリジナルとコピーを識別することができる。

【0042】また、紙媒体の場合は、複数枚のコピーを

作成すると、各コピーを物理的に識別することが可能である。しかし、電子文書の場合は、オリジナルとまったく同じ内容のコピーとして存在するため、各コピーを識別することはおろか、オリジナルと区別することもできない。

【0043】これらのことから、電子原本のオリジナルとコピーの管理には、以下のような要件が要求される。

1. 電子原本のオリジナルとコピーを一意に指し示す手段を利用者に提供する。オリジナルとコピーを識別する情報を利用者に提供し、コピーがどの電子原本のオリジナルからのコピーであるかを識別可能にする。
2. 複数回コピーをしても、各々のコピーを一意に識別可能である。

【0044】これらの要件を満たすために、SAは、次のようなオリジナルとコピーの管理を行う。

1. 文書レコードによる電子原本のオリジナルとコピーの一意識別

SAに電子文書を登録し、登録時に発行される文書レコードが指し示すSA内の電子文書が原本であり、その電子原本のみから原本のコピーを生成するように管理する。また、コピー生成時にも文書レコードを発行し、その文書レコードが指し示すSA内の電子文書のみを原本のコピーとして扱う。

【0045】文書レコードが指し示す電子文書が電子原本あるいはそのコピーであるものとして管理することにより、たとえ、利用者側で文書レコードのコピーを行ったとしても、その文書レコードはSA内の原本を一意に識別することが可能となる。したがって、どれが原本であるかわからないという問題やコピーの氾濫等の問題を解決することができる。

2. タイプ属性による管理

SAに登録する電子原本に、オリジナルとコピーを識別する属性（タイプ属性）を与える。また、原本のコピー生成の際には、原本系列IDとタイムスタンプを継承する電子文書を生成し、タイプ属性としてコピーを与え、この電子文書を原本のコピーとする。このようにして生成された電子原本のコピーは、どの電子原本のインスタンスから生成されたコピーであることを明確に示している。タイプ属性は、文書レコードに付加されて利用者へ通知され、利用者は文書レコードを参照することにより、電子原本のオリジナルとコピーを識別する。

【0046】また、電子原本のコピーには、何回目のコピーかを示す追番を含むタイプ属性を与え、複数回コピーしたとしても、各々のコピーを独立した文書として識別可能にする。この追番は、文書レコードに付加されて利用者へ通知され、利用者は個々の電子原本のコピーをそれぞれ独立したものとして識別する。こうして、追番を含むタイプ属性により、複数のコピーが管理される。

【0047】図9は、電子原本のオリジナルとコピーを文書レコードを用いて一意に識別する様子を示してい

る。電子文書D1が電子原本としてSAに登録されると、電子原本O1（オリジナル）としてSA内に保持される。そして、その電子原本に対して、文書レコードR1（オリジナル）が発行される。

【0048】この文書レコードR1は、SA内の電子原本O1を一意に識別する。また、この文書レコードR1が利用者のパーソナルコンピュータ等でコピーされたとしても、文書レコードR1のコピーはSA内の電子原本O1を一意に指し示しているため、どれが本物の原本であるかわからなくなるという問題は生じない。

【0049】次に、電子原本O1に対して、原本のコピーである電子原本O2（コピー）が生成されると、電子原本O2に対しても、電子原本O1と同様に、文書レコードR2が発行される。この文書レコードR2がコピーされたとしても、文書レコードR2のコピーはSA内の電子原本O2を一意に識別することができる。

【0050】なお、利用者側での電子文書D1のコピーは、通常のコピー操作であり、コピー先の電子文書D1-Cは原本としての効力を持たない。なぜなら、利用者のシステムでは、あくまでも、文書レコードR1が唯一に指し示すSA内の電子文書を原本として管理しているからである。

【0051】このような電子原本のオリジナルとコピーの管理によれば、たとえ、SA内の電子原本が不正に都合良く更新されたりしても、利用者のシステムは、SA内での原本の最新の状態や原本として有効なインスタンスを、文書レコードにより取り出すことができる。したがって、電子原本のオリジナルとコピーに対して、一意識別可能という安全性が与えられる。

【0052】図10は、電子文書にタイプ属性が割り振られる様子を示している。電子文書D1がSAに原本として登録される際、原本系列IDとしてSID1が与えられ、タイムスタンプとしてT1が与えられるとともに、タイプ属性としてオリジナルが与えられ、電子原本（オリジナル）として登録される。利用者がSAに登録する電子文書には、すべて、タイプ属性の初期値としてオリジナルが設定される。この登録時には、SAは、電子原本の文書レコードR1（オリジナル）を利用者に対して発行する。

【0053】そして、利用者が電子原本のコピー生成をSAに要求すると、SAは、電子原本の原本系列IDとタイムスタンプを継承し、タイプ属性をコピーに変更した電子原本（コピー）を新たに生成する。原本系列IDとタイムスタンプを継承するのは、どの時点のインスタンスのコピーであることを明確に識別するためである。そして、SAは、電子原本（オリジナル）の場合と同様に、文書レコードR2（コピー）を利用者に発行する。

【0054】図11は、タイプ属性に与える追番により、複数存在する原本のコピーの各々を独立して管理し、利用者がそれらを一意に識別する様子を示してい

る。利用者が電子原本（オリジナル）のコピー生成を要求すると、SAは、図9と同様の処理により、電子原本（コピー（1））を生成する。この時、タイプ属性のコピーには追番（1）が与えられる。

【0055】利用者が、再度、電子原本のコピー生成を要求すると、電子原本（コピー（2））が生成され、タイプ属性のコピーに追番（2）が与えられる。また、利用者には、電子原本のコピー（1）、コピー（2）に対して、それぞれ、文書レコードR2、R3が発行される。このように、タイプ属性のコピーに追番を与えることにより、SA内で各々の電子原本のコピーを独立に管理することが可能となる。また、利用者は、文書レコードを用いて、各々の電子原本のコピーを一意に識別することが可能となる。

【0056】次に、文書の物理的な所在の管理について説明する。紙媒体は、移動すると元の場所からなくなってしまうため、原本が物理的にどこにあるかを認識することは可能である。しかし、原本管理簿等で原本の所在を管理しても、その原本があるべき場所（所在）を保証することができなかった。電子文書も紙媒体と同様に、

1. 電子文書の所在を一意に特定できない。
2. コピーや移動が簡単に行うことが可能なため、不正コピーや盗難を検出することができない。

【0057】そこで、SAは、電子原本に対して以下のような処理を行い、電子原本の所在を保証する。

1. SAに登録する電子原本に、物理的に所在を特定する情報（物理ID）を与えて、所在を一意に特定する。
2. 物理IDを用いて不正コピーの検出を行う。

【0058】ネットワークやオフラインシステムが混在する環境において、複数のSAが電子原本を管理することが予想される。そこで、物理IDは、SAを特定するSA-IDとSA内のどの媒体のどの位置に保管しているかを示すアドレスIDから構成する。アドレスIDとしては、例えば、媒体上の物理アドレスが用いられる。

【0059】図12は、物理IDにより電子原本の所在を特定し、不正コピーを検出する様子を示している。電子文書D1の物理IDであるPID1は、SA-IDと文書保管部36のアドレスID（AID1）から構成され、その物理IDが電子文書D1に付加されている。電子文書D2と電子文書D3は、それぞれ、AID2とAID3をアドレスIDとして正常に保管されている電子原本である。

【0060】物理IDのテーブルは、図4の物理ID作成部37に保持され、各電子文書とそのアドレスIDから生成された物理IDの対応関係を格納している。電子文書D1、D2、D3の物理IDは、それぞれ、PID1、PID2、PID3である。

【0061】ここで、管理者等が電子文書D1を不正にコピーすると、コピーの電子文書D1-Cは、AID4

をアドレスIDとする場所に保管される。この場合、電子文書D1-Cが持つ物理IDはPID1であり、物理IDのテーブルに登録される物理IDはSA-IDとAID4から構成されるPID4である。したがって、両者の物理IDを比較すれば、それらが異なることがわかり、不正コピーが検出される。なお、別のSAに不正コピーされた場合には、SA-IDが異なるため、同様にして不正コピーが検出される。

【0062】次に、図13は、原本系列における各種識別情報の変化の例を示している。図13では、以下のような手順で識別情報が変更される。

P1：登録

時刻T1において、利用者は、SA1に電子文書D1-1を登録する。SA1は、登録の処理として、第1に、SID1を原本系列IDとして割り振る。この原本系列IDにより、原本の状態の変化していく系列が一意に識別される。第2に、タイムスタンプとしてT1を割り振る。このタイムスタンプにより、原本系列での各時点のインスタンスが一意に識別される。第3に、タイプ属性としてオリジナルを設定する。SAに登録される電子文書のタイプ属性は、すべて、オリジナルである。

【0063】そして、SA1は、これらの識別情報、すなわち、原本系列ID、タイムスタンプ、およびタイプ属性により、各時点での原本を論理的に一意に識別する。また、第4に、物理IDとしてPID1を割り振る。この物理IDにより、電子文書の所在を明確にし、不正コピーの検出等を行う。

P2：更新（状態変化）

時刻T2において、利用者は、電子文書D1-1を更新し、電子文書D1-2を生成する。これにより、原本の状態が変化する。このとき、原本系列IDとタイプ属性は変更されず、新たなタイムスタンプと物理IDとして、それぞれ、T2とPID2が割り振られた電子原本が作成される。

P3：コピー作成

利用者は、電子文書D1-2のコピーを作成する。このとき、原本系列IDとタイムスタンプは変更されず、新たなタイプ属性と物理IDとして、それぞれ、コピー（1）とPID3が割り振られた電子原本が作成される。タイムスタンプを変更しないのは、原本系列のある時点のコピーであることを明確に識別するためである。コピーを作成した時刻は、履歴等の管理情報として保持される。また、コピー属性には追番が振られ、個々のコピーのインスタンスが管理される。

P4：移動

時刻T3において、利用者は、電子文書D1-2をSA1からSA2に移動する。このとき、原本系列IDとタイプ属性は変更されず、新たなタイムスタンプと物理IDとして、それぞれ、T3とPID4が割り振られた電子原本が作成される。物理IDにはSAを一意に識別す

るIDが含まれているので、これを用いて不当な電子文書の移動を検出することができる。

【0064】次に、SA内で行われる処理についてより詳細に説明する。図14は、識別IDの生成の様子を示している。ここでは、以下のような手順で処理が行われる。

P1：論理識別ID作成要求

電子文書の登録要求を受けると、原本系列管理部34は、論理識別ID作成要求をセキュリティハードウェアに対して行う。

P2：要求

要求時に、原本系列管理部34は、オリジナル原本に対する要求か、コピー原本に対する要求かを指定するタイプ属性をセキュリティハードウェアに対して与える。また、コピー原本の場合には、コピー元のオリジナル原本の論理識別IDも与える。

P3：論理識別ID生成

セキュリティハードウェアは、図4の暗号処理部38、鍵保持部39、識別ID作成部40、時刻生成部41、装置ID保持部42、およびインクリメンタルカウンタ43を含む。

【0065】識別ID作成部40は、装置ID保持部42が保持している装置IDとインクリメンタルカウンタ43が保持しているカウンタ値から原本系列ID61を生成し、時刻生成部41内のリアルタイムクロック(RTC)が出力する時刻からタイムスタンプ63を生成する。そして、これらの情報を原本系列管理部34が指定したタイプ属性62と連結して、論理識別IDを生成する。コピー原本の場合には、与えられたオリジナル原本の論理識別IDに含まれる原本系列IDとタイムスタンプを継承して、論理識別IDを生成する。

P4：SAの署名

暗号処理部38は、鍵保持部39に保持されているSAの個別鍵64を用いて、P3で連結された情報に対してSAのデジタル署名を生成する。SAのデジタル署名は、SAの個別鍵64で作成するMAC(Message Authentication Code)に対応する。暗号処理部38は、P3で連結された情報にこのMACの値を連結して、電子文書を論理的に識別する最終的な論理識別ID66を生成する。図14において、円で囲まれたSAは、生成された情報がSAのデジタル署名を含むことを表している。

P5：論理識別ID返答

暗号処理部38は、論理識別ID66を、論理識別ID作成要求に対するセキュリティハードウェアの処理結果として、原本系列管理部34に返す。

P6：電子文書保管

ファイルシステムは、文書保管部36と物理ID作成部37を含む。原本系列管理部34は、返された論理識別ID66をファイル名として、電子文書をファイルシ

テム内の文書保管部36に格納する。

P7：識別ID作成要求

原本系列管理部34は、識別ID作成要求をセキュリティハードウェアに対して行う。このとき、物理ID作成部37から物理ID67を取得し、論理識別ID66と物理ID67をセキュリティハードウェアに与える。

P8：SAの署名

暗号処理部38は、SAの個別鍵64を用いて、論理識別ID66と物理ID67を連結した情報に対してSAの署名を生成する。そして、論理識別ID66と物理ID67を連結した情報にSAの署名を連結して、識別ID68を生成する

P9：識別ID返答

暗号処理部38は、識別ID作成要求に対するセキュリティハードウェアの処理結果として、識別ID68を返す。

P10：識別IDを管理情報に格納

識別ID68を電子原本の管理情報として格納する。

【0066】図15は、SA内で電子文書を保管する様子を示している。ここでは、以下のような手順で処理が行われる。

P1：原本系列管理部34は、クライアントから電子文書71と登録情報72を取得し、セキュリティハードウェアに識別IDの生成を指示する。登録情報72には、利用者IDと利用者の電子文書名が含まれる。

P2：セキュリティハードウェアは、識別ID68を生成して、原本系列管理部34に返す。

P3：原本系列管理部34は、電子文書71、登録情報72、および管理情報73を識別ID68に関連付け、これらの情報を連結する。管理情報73には、SAの接続先情報が含まれる。

P4：原本系列管理部34は、セキュリティハードウェアに改ざん検出情報の生成を指示する。このとき、電子文書71、登録情報72、および管理情報73を連結した情報を、セキュリティハードウェアに与える。

P5：セキュリティハードウェアは、受け取った情報に対して、SAの個別鍵64を用いてSAの署名を生成する。そして、それを改ざん検出情報として管理情報に付加し、電子原本74を生成する。

P6：セキュリティハードウェアは、電子原本74を処理結果として返す。

P7：原本系列管理部34は、電子原本74を原本のオリジナルとして、ファイルシステムに登録する。

【0067】図16は、文書レコード生成の様子を示している。ここでは、以下のような手順で処理が行われる。

P1：文書レコード情報整形

原本系列管理部34は、電子原本74の管理情報から、識別IDとSAの接続先情報を取得し、電子原本74の登録情報から、利用者IDと利用者の電子文書名を取得

して、取得した情報を図4の登録証書作成部35に渡す。登録証書作成部35は、受け取った情報を文書レコード情報81として整形し、原本系列管理部34に返す。

P2：文書レコード作成指示

原本系列管理部34は、電子文書71と文書レコード情報81をセキュリティハードウェアに与えて、文書レコードの作成を指示する。

P3：ハッシュ値計算

セキュリティハードウェア内の暗号処理部38は、電子文書71のハッシュ値82を計算する。

P4：ハッシュ値連結

暗号処理部38は、ハッシュ値82を文書レコード情報81に連結する。

P5：改ざん検出情報生成

暗号処理部38は、図15の処理と同様に、SAの個別鍵64を用いて改ざん検出情報を生成し、改ざん検出情報を文書レコード情報81に連結して、文書レコード83を生成する。

P6：文書レコード返答

暗号処理部38は、文書レコード83を処理結果として原本系列管理部34に返す。

P7：原本系列管理部34は、文書レコード83をクライアントに送信する。

【0068】次に、SAの基本機能である登録、検索、文書レコード検証、同一性検証、更新、移動、チェックアウト・チェックイン、および状態遷移取得について説明する。

【0069】図17は、電子文書の登録の様子を示している。登録とは、クライアントが生成した電子文書をSAに原本として登録することである。ここでは、以下のような手順で処理が行われる。

P1：クライアントは、ファイル名91の電子文書71を作成し、社外秘等の属性や保管期間のように、サービスに依存する情報を登録情報72として作成する。

P2：クライアントは、ファイル名91、電子文書71、および登録情報72を、クライアントとSAの間のセッション鍵で暗号化して、SAに送信する。図17において、円で囲まれた文字“セ”は、情報がセッション鍵により暗号化されていることを表している。

P3：SAは、受け取った情報を復号化し、電子文書71に対して、識別IDと、作成日時や改ざん検出情報等を含む管理情報を自動生成し、生成した情報を電子文書71および登録情報72と連結して、原本のオリジナル74を生成する。

P4：SAは、登録の結果として、文書レコード83を発行する。文書レコード83には、図16に示したような情報が含まれている。このうち、SAの接続先情報としては、例えば、SAのエイリアス(alias)名が用いられる。基本的には、この文書レコード83を用いて他

の処理が行われる。

P5：SAは、文書レコード83をセッション鍵で暗号化して、クライアントに通知する。

P6：クライアントは、受け取った情報を復号化し、ファイル名91に文書レコード83を関連付けて、情報を更新する。

【0070】図18は、電子文書の検索(参照)の様子を示している。検索とは、SAに保管されている電子文書を文書レコードの情報(識別ID)をキーとして取り出すことである。ここでは、以下のような手順で処理が行われる。

P1：クライアントは、検索対象の電子文書の文書レコード83を選択し、接続先情報からアクセスするSAを確認する。

P2：クライアントは、文書レコード83をSAに送付する。

P3：SAは、文書レコード83の識別IDをキーとして、原本74を検索する。

P4：SAは、検索された原本74の電子文書をクライアントに通知する。

P5：クライアントは、受け取った電子文書をファイル名91に関連付けて、情報を更新する。

【0071】図19は、文書レコードの検証の様子を示している。文書レコード検証とは、クライアントに保持されている文書レコードが最新のものであるか否かを検証することである。図19では、SA内の電子原本の状態が更新等により変化しており、最新の文書レコードが新たに通知されている。ここでは、以下のような手順で処理が行われる。

P1：クライアントは、検証対象の電子文書を選択する。ここでは、ファイル名92の電子文書93が選択されている。

P2：クライアントは、電子文書93の文書レコード94をSAに送付する。

P3：SAは、クライアントから送られてきた文書レコード94の識別IDから原本系列IDを取り出し、その原本系列IDに対応する原本系列の中でタイムスタンプが最新の電子原本95を検索する。そして、電子原本95の識別IDと文書レコード94の識別IDを比較する。両者が一致すれば、文書レコード94は最新のものであることがわかり、両者が一致しなければ、電子原本の状態が変化していることがわかる。

P4：SAは、電子原本の状態が変化していることを検出し、最新の文書レコード96を作成する。

P5：SAは、最新の文書レコード96をクライアントに通知する。

P6：クライアントは、通知された文書レコード96をファイル名91に関連付け、情報を更新する。その後、最新の電子文書を取得する場合には、文書レコード96を用いて、図18の検索処理により電子文書を取得す

る。

【0072】図20は、同一性検証の様子を示している。同一性検証とは、クライアントが保存している電子文書とSA内の電子原本とが同一であるか否かを検証することである。ここでは、以下のような手順で処理が行われる。

P1：クライアントは、検証対象の電子文書93と文書レコード94を選択する。

P2：クライアントは、文書レコード94と電子文書93をSAに送付する。

P3：SAは、クライアントから送られてきた電子文書93の改ざん検出情報を計算し、文書レコード94が指し示すSA内の電子原本97の改ざん検出情報と比較して、両者が同一か否かを検証する。

P4：SAは、検証結果98に署名を行って、クライアントに通知する。

P5：クライアントは、検証結果98を確認する。

【0073】図21は、電子文書の更新の様子を示している。更新とは、SA内の電子文書に対応するクライアント内の電子文書を、更新文書としてSA内の電子文書に関連付けることである。ここでは、以下のような手順で処理が行われる。

P1：クライアントは、更新文書として電子文書D2を作成し、更新対象の電子文書D1の文書レコードR1、電子文書D2、および電子文書D2に関わる登録情報G2を選択する。

P2：クライアントは、文書レコードR1、電子文書D2、および登録情報G2をSAに送付する。

P3：SAは、文書レコードR1に対応する電子原本O1を取得し、その識別IDであるID1のタイムスタンプ部分を更新して、新たな識別IDとしてID2を生成する。そして、電子文書D2をID2に関連付けて登録し、電子原本O2を生成する。このとき、電子原本O1の管理情報M1、登録情報G1は更新されて、それぞれ、管理情報M2、登録情報G3となる。登録情報G3は、登録情報G1と登録情報G2を含む。

P4：SAは、更新された電子原本O2の文書レコードR2を作成する。

P5：SAは、文書レコードR2をクライアントに通知する。

P6：クライアントは、文書レコードR2を電子文書D2のファイル名に関連付けて、情報を更新する。

【0074】図22および図23は、電子文書の移動の様子を示している。移動とは、SA内の電子文書を他のSAに移動することである。移動元の電子文書の情報は、サービス形態に応じて、残される場合と消去される場合とがある。ここでは、移動元の電子文書の情報を残すものとし、以下のような手順で処理が行われる。

P1：クライアントは、移動する電子文書D1と移動先SAを選択する。移動先SAのリストは、必要に応じ

て、移動元SAから示される。

P2：クライアントは、電子文書D1の文書レコードR1と移動先SAを指定する情報101を、移動元SAに送付する。

P3：移動元SAは、文書レコードR1が指し示す電子原本O1の電子文書D1に対するエクスポート処理を行う。まず、識別IDがID1である電子文書D1、管理情報M1、および登録情報G1を連結する。次に、連結データに対して、移動先SAと移動元SAが共有している共通鍵（個別共有鍵、グループ共有鍵等）を用いて、改ざん検出情報を生成する。そして、改ざん検出情報を元の連結データと連結して、バックドデータ102を生成する。

P4：移動元SAは、バックドデータ102を移動先SAに送付する。

P5：移動先SAは、バックドデータ102の改ざんの有無を検証し、インポート処理を行う。この処理では、バックドデータ102をアンパックして、電子文書D1、管理情報M1、および登録情報G1を取り出す。

P6：移動先SAは、ID1のタイムスタンプと物理IDを更新して、タイムスタンプと物理IDが異なる識別IDであるID2を生成する。

P7：移動先SAは、3ウェイハンドシェークによる否認防止の処理として、否認防止レコード103とID2を移動元SAに送付する。

P8：移動元SAは、受け取ったID2のタイムスタンプを更新してID3を生成し、ID3に関連付けて、電子文書D1のハッシュ値104を移動した電子文書の情報（電子原本O3）として登録する。電子原本O3には、移動先の識別IDであるID2が付加された管理情報M3と、登録情報G1が含まれる。

P9：移動元SAは、3ウェイハンドシェークによる否認防止の処理として、否認防止レコード103を移動先SAに送付する。

P10：移動先SAは、ID2に関連付けて、電子文書D1を移動してきた電子文書（電子原本O2）として登録する。電子原本O2には、移動元の識別IDであるID1が付加された管理情報M2と、登録情報G1が含まれる。

P11：移動元SAは、ID2の情報を含む文書レコードR3を生成する。

P12：移動元SAは、文書レコードR3をクライアントに送信する。

P13：移動先SAは、ID1の情報を含む文書レコードR2を生成する。

P14：移動先SAは、文書レコードR2をクライアントに送信する。

P15：クライアントは、文書レコードR2、R3を電子文書D1のファイル名に関連付け、情報を更新する。

【0075】図24は、チェックアウトおよびチェック

インの様子を示している。チェックアウトとは、利用者からの要求により、SA内に登録されている原本をロックし、チェックイン要求があるまで原本の状態を変化させないようにすることである。また、チェックインとは、利用者からの要求により、原本のロックを解除することである。ここでは、以下のような手順で処理が行われる。

P1：クライアントは、チェックアウト対象の電子文書D1を選択する。

P2：クライアントは、電子文書D1の文書レコードR1をSAに送付して、チェックアウトを要求する。

P3：SAは、チェックアウト処理を行う。まず、電子文書D1を含む電子原本O1の管理情報M1にチェックアウト属性を付与し、識別IDであるID1のタイムスタンプを更新して、タイムスタンプが異なるID2を生成する。そして、チェックアウト属性を有する文書レコードR2を作成する。

P4：SAは、文書レコードR2をクライアントに通知する。

P5：クライアントは、電子文書D1を電子文書D2に更新する。この更新処理は、クライアント内だけではなく、更新機能を用いて、SA内のID2の電子文書に対して行うこともできる。また、更新処理は、複数回行ってもよい。

P6：クライアントは、文書レコードR2、最終的な電子文書D2、電子文書D2の登録情報G2をSAに送付して、チェックインを要求する。

P7：SAは、チェックイン処理を行う。まず、ID2のタイムスタンプを更新してID3を生成し、管理情報M1にチェックイン属性を付与して管理情報M2を生成する。そして、電子文書D2を電子原本O2として登録する。

P8：SAは、チェックイン属性を有する文書レコードR3を作成する。

P9：SAは、文書レコードR3をクライアントに通知する。

P10：クライアントは、文書レコードR3を電子文書D2のファイル名に関連付けて、情報を更新する。

【0076】図25は、状態遷移取得の様子を示している。状態遷移取得とは、文書レコードが指す電子原本の状態がどのように遷移したかを示す状態遷移情報を取得することである。状態遷移情報は、電子原本に対して行われた操作の履歴に対応し、管理情報の一部として保持される。ここでは、以下のような手順で処理が行われる。

P1：クライアントは、状態遷移情報を取得すべき電子文書93を選択する。

P2：クライアントは、電子文書93の文書レコード94をSAに送付する。

P3：SAは、文書レコード94が指し示すSA内の電

子原本97の最新の管理情報から、状態遷移情報105を取得する。

P4：SAは、状態遷移情報105をクライアントに通知する。

P5：クライアントは、状態遷移情報105の内容を確認する。

【0077】図26は、状態遷移情報の例を示している。この状態遷移情報には、1998年2月17日の12：00に、ユーザAがSA1に原本を登録し、14：00に、ユーザBがSA1からSA2に原本を移動し、15：00に、ユーザCが原本のコピーを作成し、16：00に、ユーザDがSA2からSA3に原本を移動したことが記録されている。したがって、利用者は、状態遷移情報を参照することで、登録時から現在までの電子原本の状態を追跡することができる。

【0078】以上説明した実施形態では、主として、電子化された重要文書を電子文書としてSAに登録しているが、それ以外にも、任意のフォーマットの任意の電子情報をSAに登録することが可能である。例えば、音声データ、画像データ、ビデオデータ等を登録しておき、電子文書と同様にして管理することができる。

【0079】ところで、図3のSA11、21、クライアント12、および端末22は、例えば、図27に示すような情報処理装置（コンピュータ）を用いて構成することができる。図27の情報処理装置は、CPU（中央処理装置）111、メモリ112、入力装置113、出力装置114、外部記憶装置115、媒体駆動装置116、およびネットワーク接続装置117を備え、それらはバス118により互いに接続されている。

【0080】メモリ112は、例えば、ROM（read only memory）、RAM（random access memory）等を含み、処理に用いられるプログラムとデータを格納する。例えば、図4に示した原本系列管理部34と登録証書作成部35は、プログラムモジュールとしてメモリ112に格納される。CPU111は、メモリ112を利用してプログラムを実行することにより、必要な処理を行う。

【0081】入力装置113は、例えば、キーボード、ポインティングデバイス、タッチパネル等であり、利用者または管理者からの指示や情報の入力に用いられる。出力装置114は、例えば、ディスプレイ、プリンタ、スピーカ等であり、利用者または管理者への問い合わせや処理結果の出力に用いられる。

【0082】外部記憶装置115は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク（magneto-optical disk）装置等である。情報処理装置は、この外部記憶装置115に、上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリ112にロードして使用することができる。また、外部記憶装置115は、図4の文書保管部36および物理ID作成部37

としても用いられる。

【0083】媒体駆動装置 116 は、可搬記録媒体 119 を駆動し、その記録内容にアクセスする。可搬記録媒体 119 としては、メモリカード、フロッピーディスク、CD-ROM (compact disk read only memory)、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体が用いられる。利用者は、この可搬記録媒体 119 に上述のプログラムとデータを格納しておき、必要に応じて、それらをメモリ 112 にロードして使用することができる。また、可搬記録媒体 119 は、図 3 のセキュア媒体 16 としても用いられる。

【0084】ネットワーク接続装置 117 は、LAN (local area network) 等の任意のネットワーク (回線) を介して外部の装置と通信し、通信に伴うデータ変換を行う。情報処理装置は、必要に応じて、上述のプログラムとデータをネットワーク接続装置 117 を介して外部の装置から受け取り、それらをメモリ 112 にロードして使用することができる。ネットワーク接続装置 117 は、例えば、図 4 のネットワークインタフェース 31 に対応する。

【0085】図 28 は、図 27 の情報処理装置にプログラムとデータを供給することのできるコンピュータ読み取り可能な記録媒体を示している。可搬記録媒体 119 や外部のデータベース 120 に保存されたプログラムとデータは、メモリ 112 にロードされる。そして、CPU 111 は、そのデータを用いてそのプログラムを実行し、必要な処理を行う。

【0086】

【発明の効果】本発明によれば、利用者が利用するコンピュータ環境とは別に、電子原本管理装置を設け、電子原本管理装置が発行する登録証書を用いて、電子文書の登録、更新、移動等の処理が行われる。これにより、電子文書に対して、紙媒体と同等以上の安全性 (原本性) を与えることが可能となる。

【図面の簡単な説明】

【図 1】本発明の電子原本管理装置の原理図である。

【図 2】電子原本モデルを示す図である。

【図 3】電子原本管理システムの構成図である。

【図 4】セキュアアーカイバの構成図である。

【図 5】セキュアアーカイバの処理のフローチャートである。

【図 6】文書レコードを示す図である。

【図 7】原本系列の管理を示す図である。

【図 8】時系列管理を示す図である。

【図 9】オリジナルとコピーの識別を示す図である。

【図 10】タイプ属性による管理を示す図である。

【図 11】複数コピーの管理を示す図である。

【図 12】不正コピーの検出を示す図である。

【図 13】識別情報の変化を示す図である。

【図 14】識別 ID の生成を示す図である。

【図 15】電子文書の保管を示す図である。

【図 16】文書レコードの生成を示す図である。

【図 17】登録処理を示す図である。

【図 18】検索処理を示す図である。

【図 19】文書レコード検証処理を示す図である。

【図 20】同一性検証処理を示す図である。

【図 21】更新処理を示す図である。

【図 22】移動処理を示す図 (その 1) である。

【図 23】移動処理を示す図 (その 2) である。

【図 24】チェックアウト・チェックイン処理を示す図である。

【図 25】状態遷移取得処理を示す図である。

【図 26】状態遷移情報を示す図である。

【図 27】情報処理装置の構成図である。

【図 28】記録媒体を示す図である。

【符号の説明】

1 登録手段

2 付与手段

3 管理手段

4 発行手段

11、21 セキュアアーカイバ

12 サービスクライアント

13 ローカルな環境

14、74、95、97、O1、O2、O3 電子原本

15、83、94、96、R1、R2、R3 文書レコード

16 セキュア媒体

22 利用者端末

31 ネットワークインタフェース

32 要求解釈部

33 返答作成部

34 原本系列管理部

35 登録証書作成部

36 文書保管部

37 物理 ID 作成部

38 暗号処理部

39 鍵保持部

40 識別 ID 作成部

41 時刻生成部

42 装置 ID 保持部

43 インクリメンタルカウンタ

51、82、104 ハッシュ値

52、68 識別 ID

53 利用者側の電子文書名

54 利用者 ID

55 SA の接続先情報

56 SA の署名

61、SID1、SID2 原本系列 ID

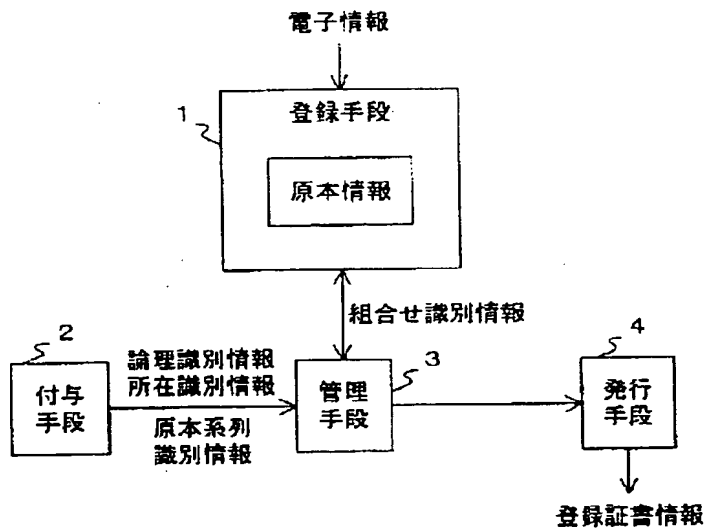
62 タイプ属性

63 T1、T2、T3、T4、T5 タイムスタンプ
 64 SAの個別鍵
 66 論理識別ID
 67、PID1、PID2、PID3、PID4 物理ID
 71、93、D1、D1-1、D1-2、D1-3、D1-4、D1-5、D1-C、D2、D2-1、D2-2、D2-3、D2-4、D2-5 電子文書
 72、G1、G2、G3 登録情報
 73、M1、M2、M3 管理情報
 81 文書レコード情報
 91、92 ファイル名
 98 検証結果
 101 移動先SAの情報
 102 パックドデータ

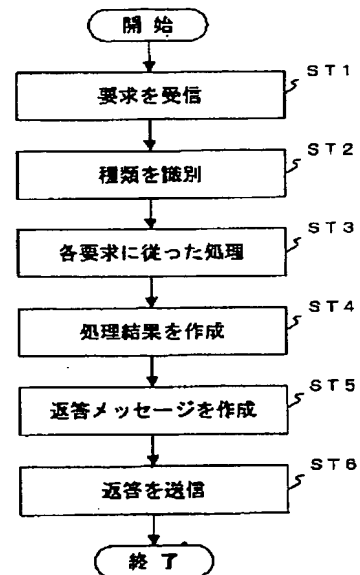
103 否認防止レコード
 105 状態遷移情報
 111 CPU
 112 メモリ
 113 入力装置
 114 出力装置
 115 外部記憶装置
 116 媒体駆動装置
 117 ネットワーク接続装置
 10 119 可搬記録媒体
 120 データベース
 S1、S2 原本系列
 AID1、AID2、AID3、AID4 アドレスID

【図1】

本発明の原理図

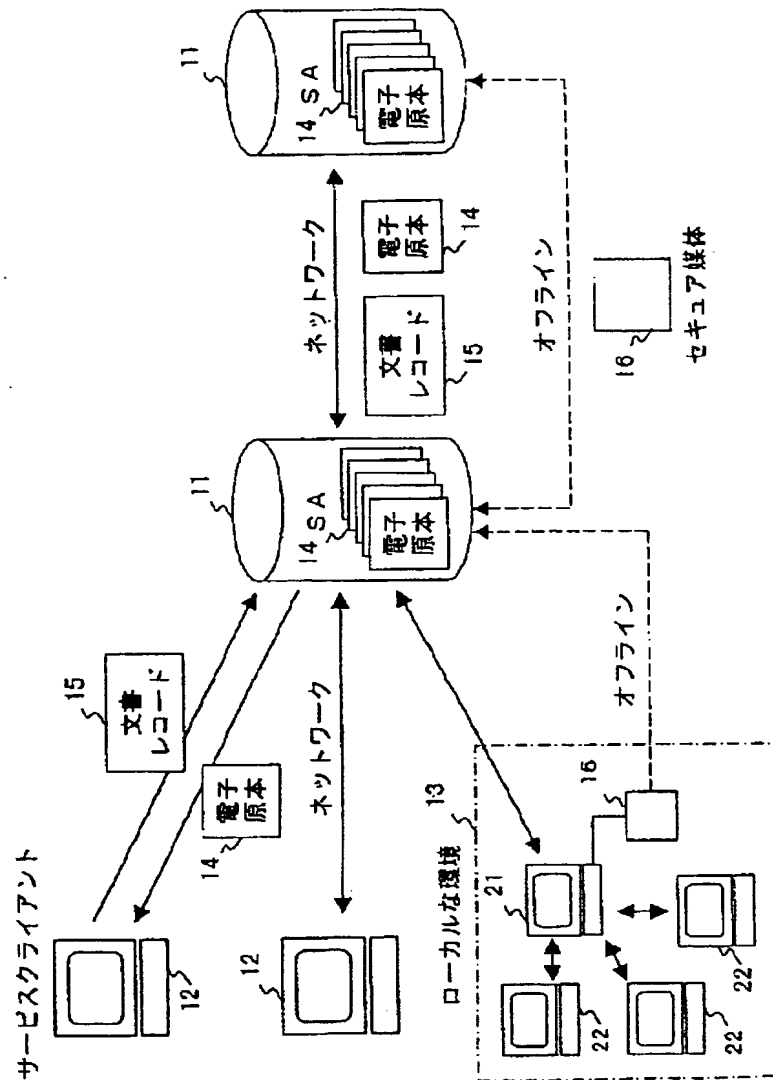


【図5】

セキュアアーカイバの
処理のフローチャート

【図3】

電子原本管理システムの構成図



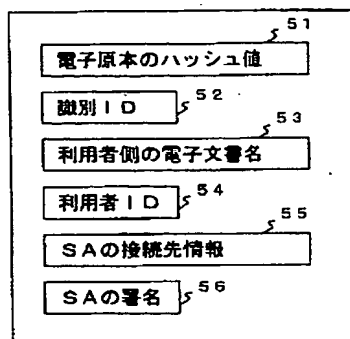
【図26】

状態遷移情報を示す図

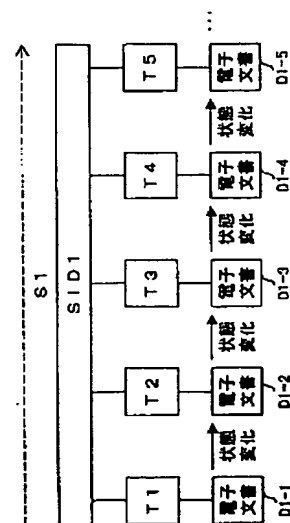
1998年2月17日: 12:00: ユーザA: 登録: SA1: ID11223344
1998年2月17日: 14:00: ユーザB: 原本移動: SA1: SA2
1998年2月17日: 15:00: ユーザC: コピー作成
1998年2月17日: 16:00: ユーザD: 原本移動: SA2: SA3

【図6】

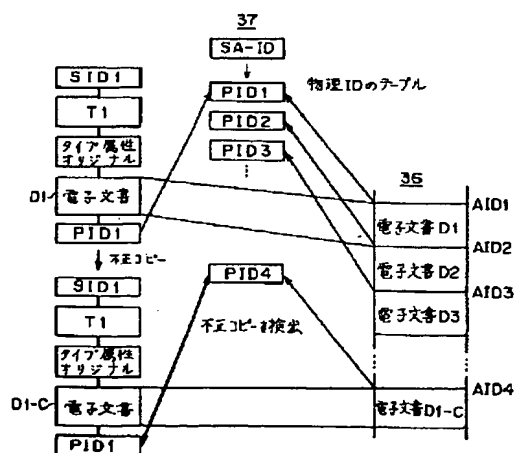
文書レコードを示す図



時系列管理を示す図

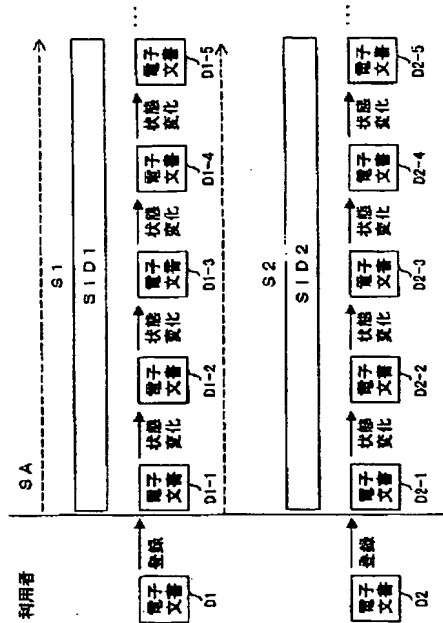


不正コピーの検出を示す図



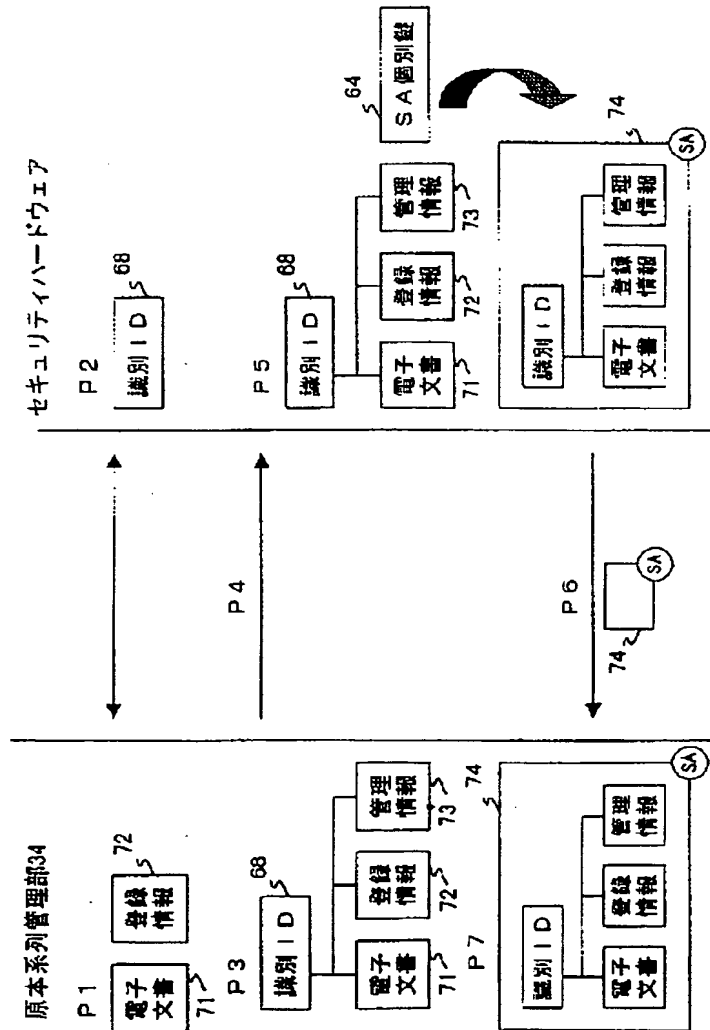
【図7】

原本系列の管理を示す図



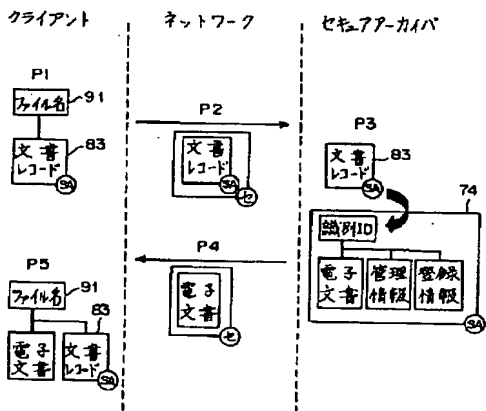
【図15】

電子文書の保管を示す図



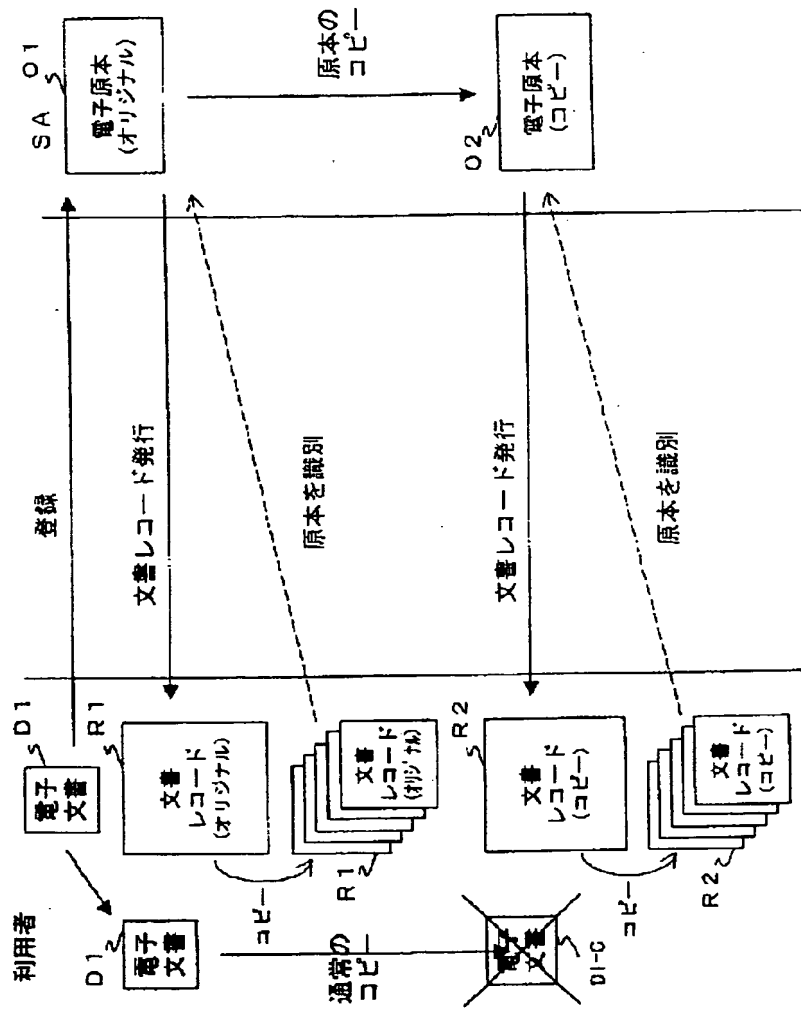
【図18】

検索処理を示す図



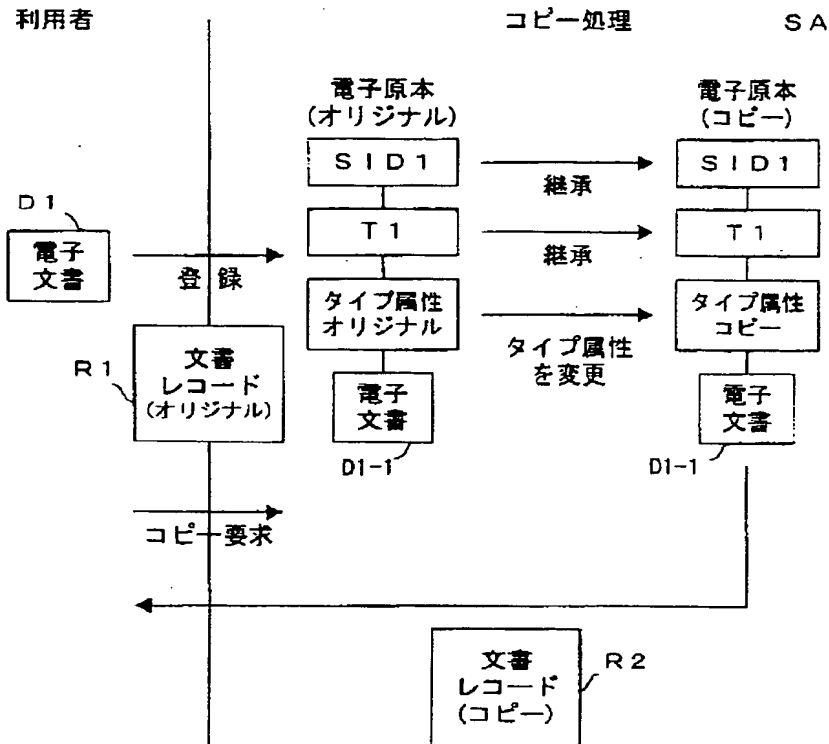
【図9】

オリジナルとコピーの識別を示す図



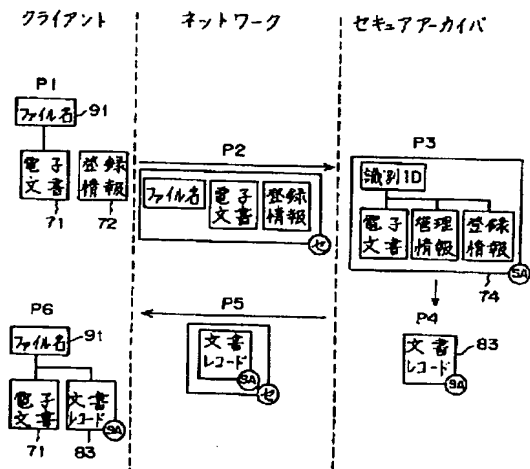
【図10】

タイプ属性による管理を示す図



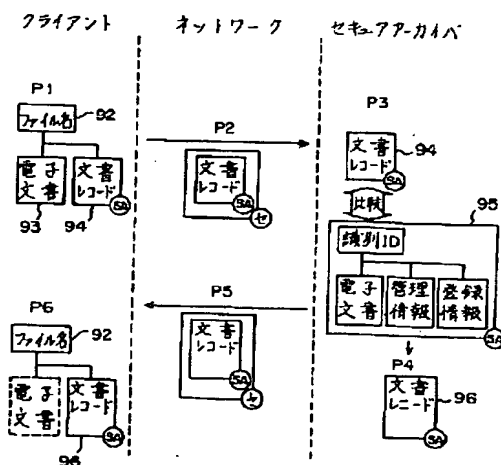
【図17】

登録処理を示す図



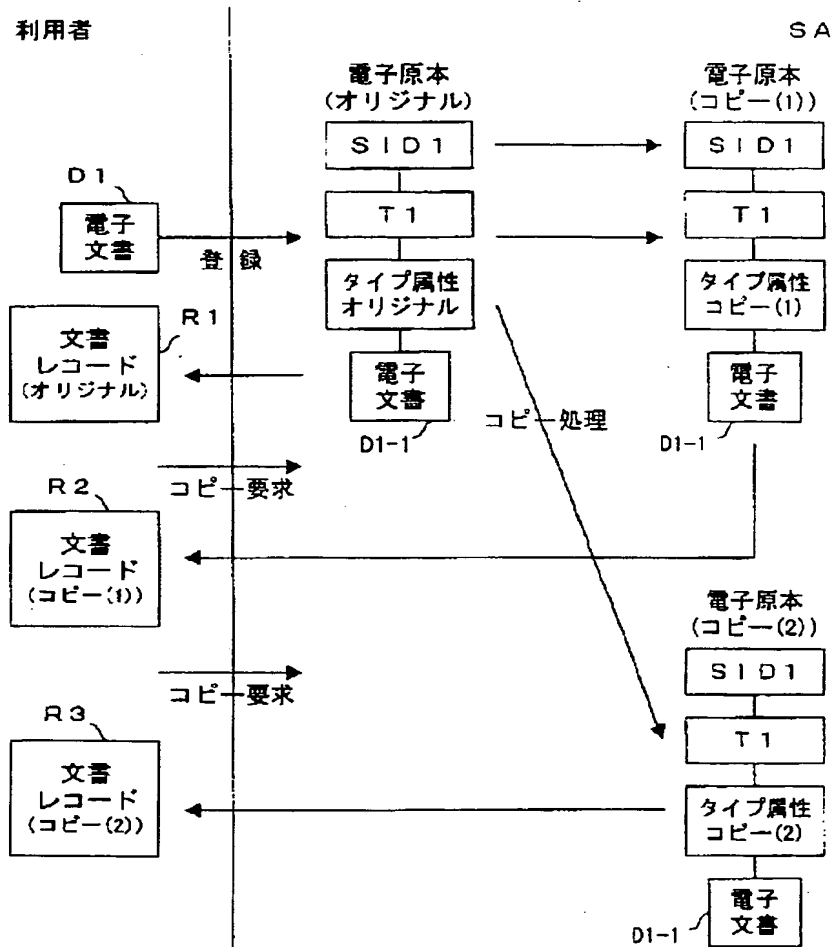
【図19】

文書レコード検証処理を示す図



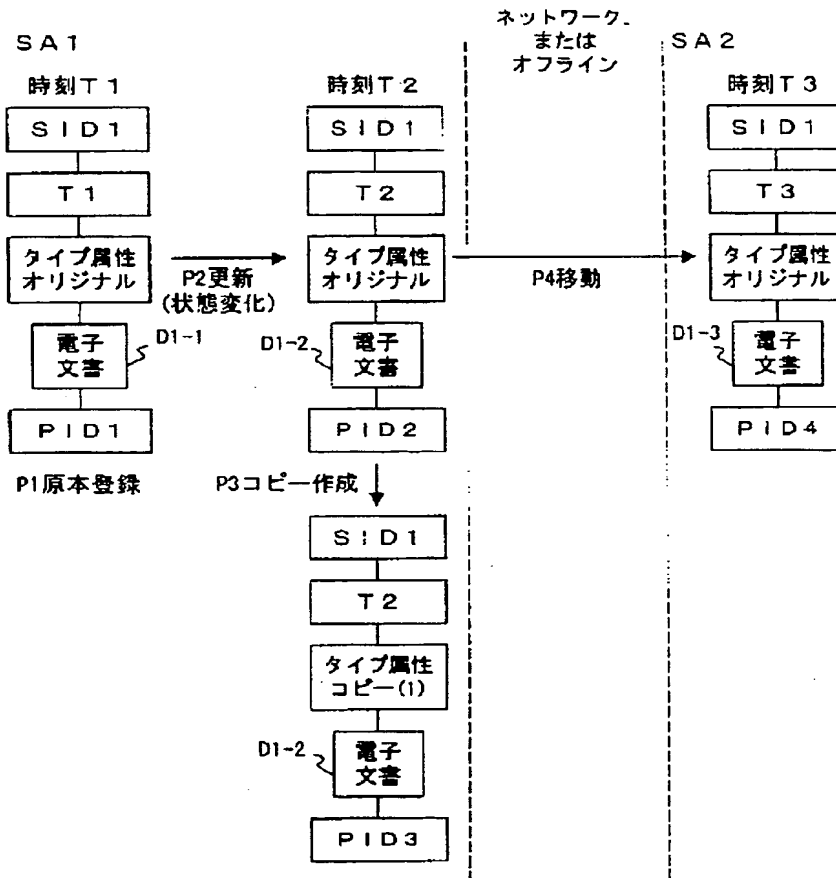
【図11】

複数コピーの管理を示す図



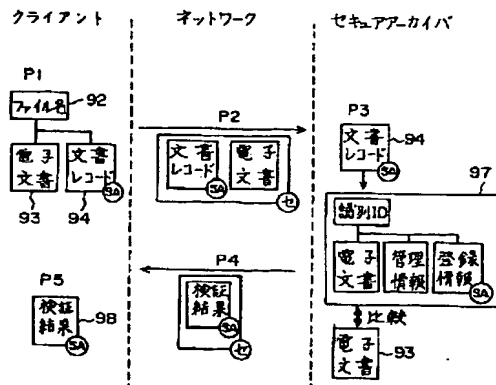
【図13】

識別情報の変化を示す図

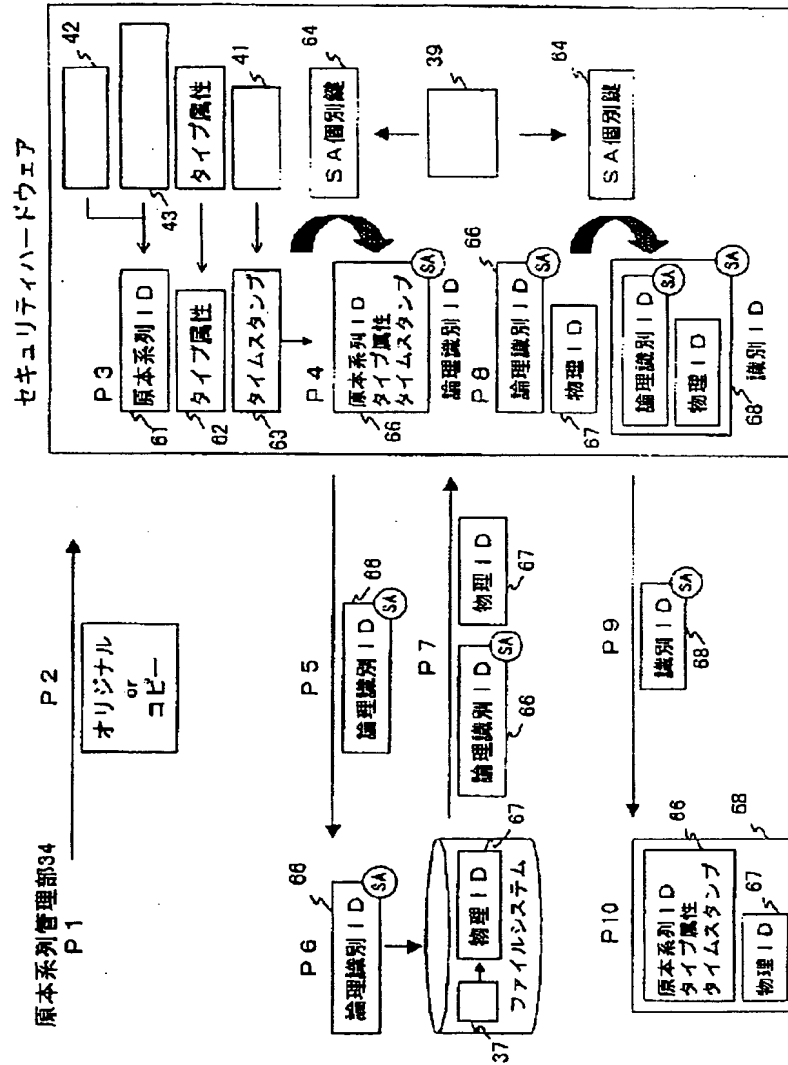


【図20】

同一性検証処理を示す図

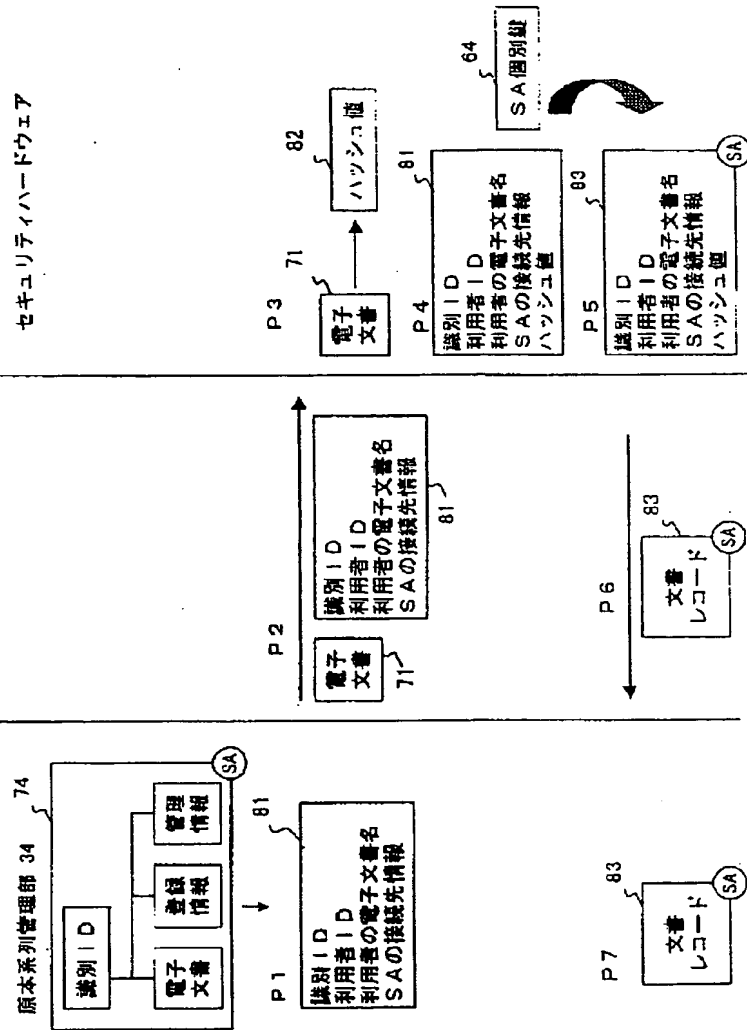


識別 ID の生成を示す図



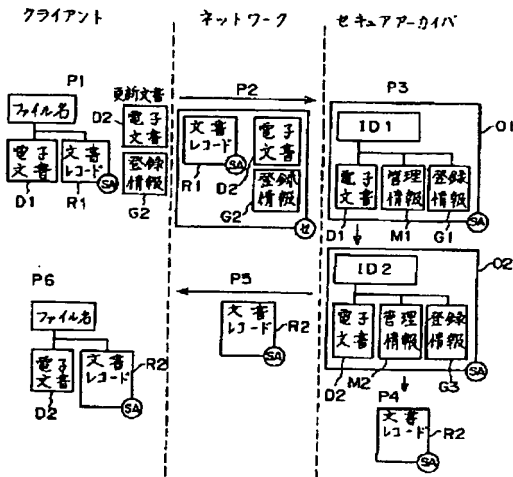
【図16】

文書レコードの生成を示す図



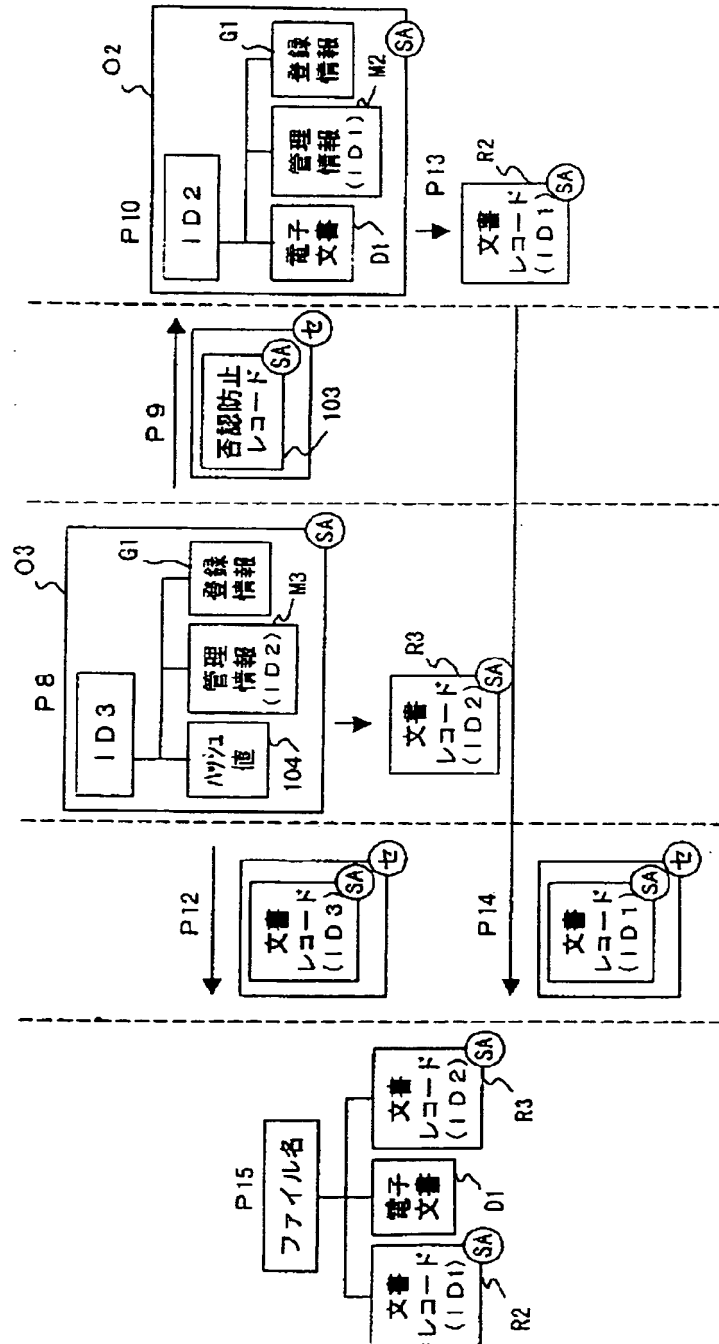
【図21】

更新処理を示す図



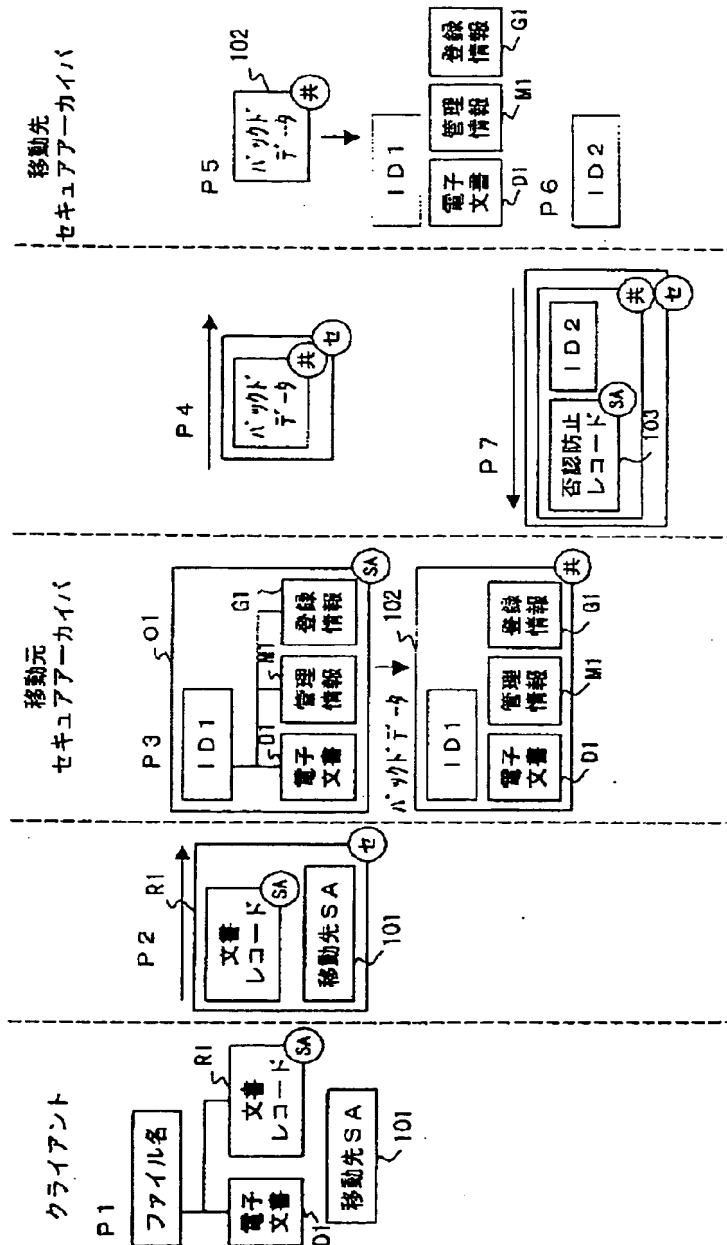
【図23】

移動処理を示す図 (その2)



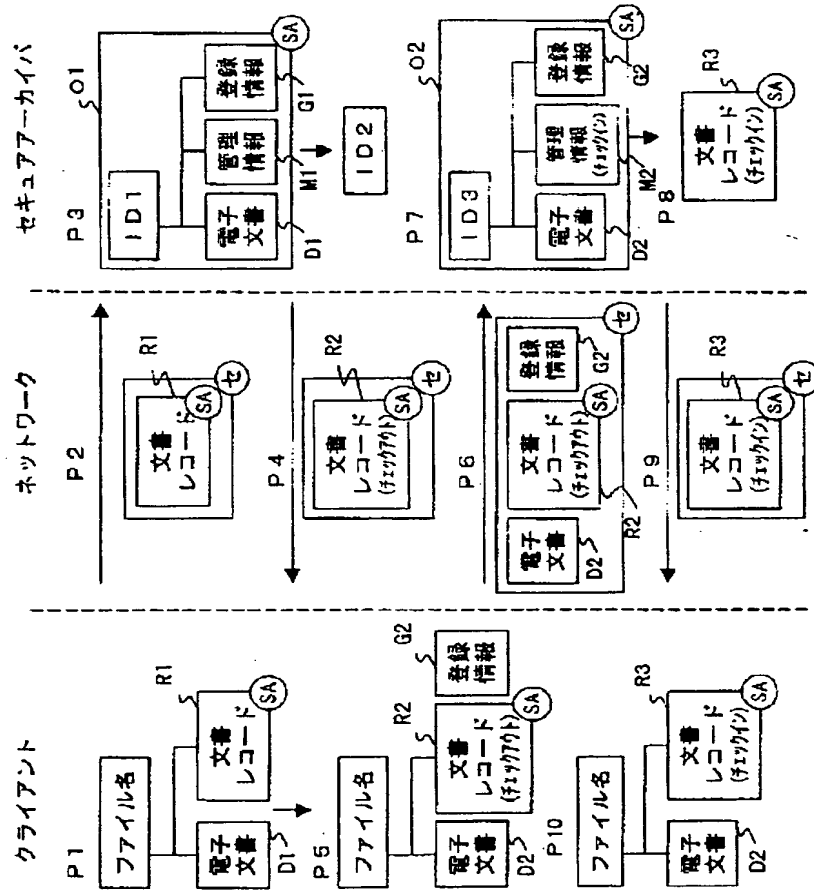
【図22】

移動処理を示す図（その1）



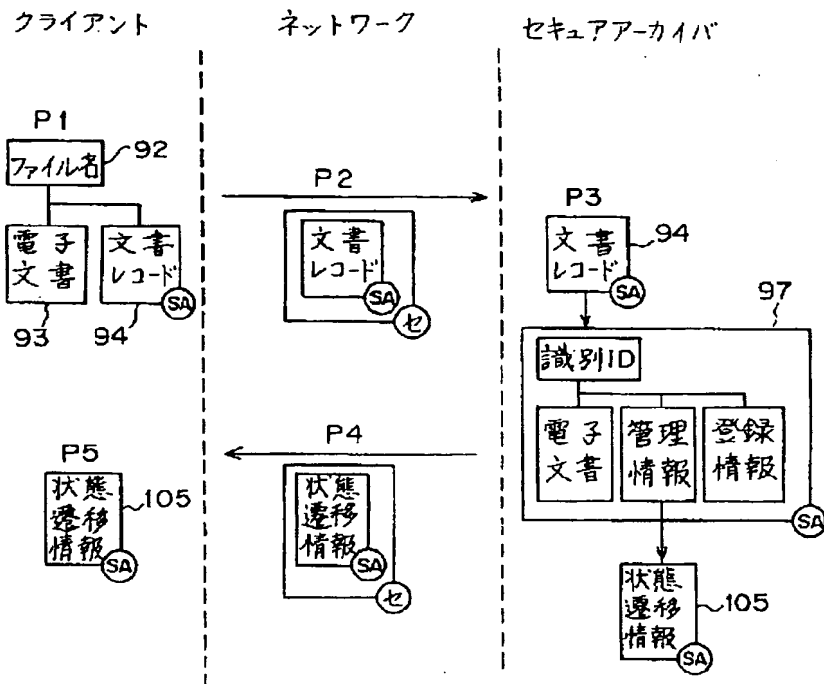
【図24】

チェックアウト・チェックイン処理を示す図



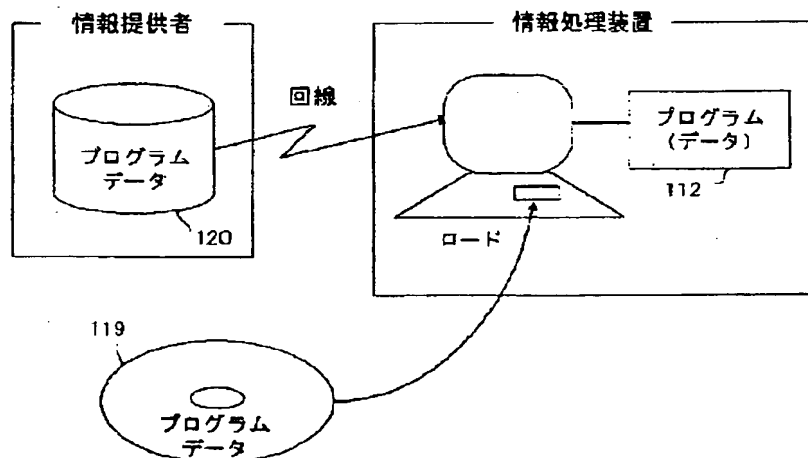
【図25】

状態遷移取得処理を示す図



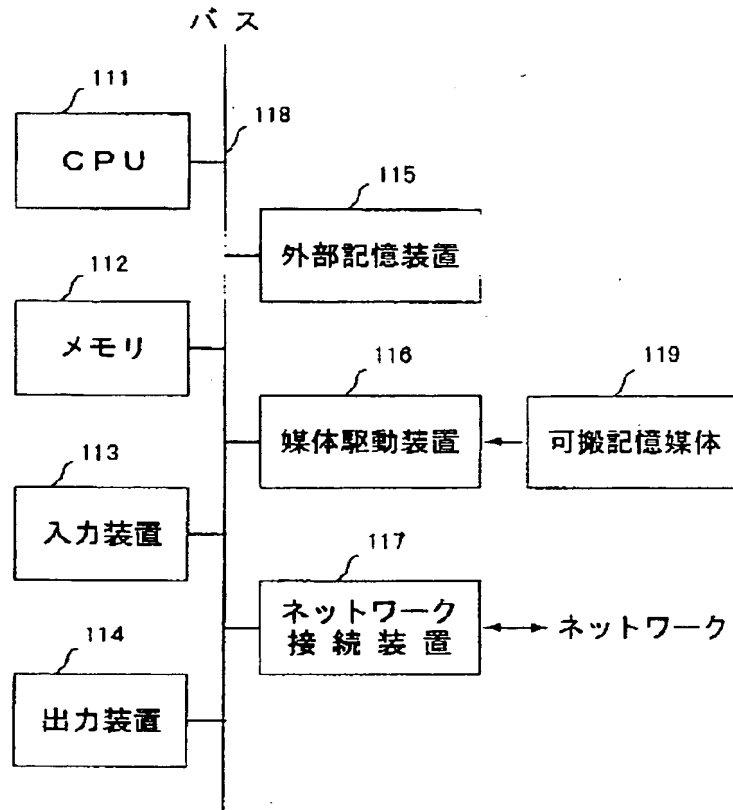
【図28】

記憶媒体を示す図



【図27】

情報処理装置の構成図



フロントページの続き

(72)発明者 小野 越夫
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

Fターム(参考) 5B017 AA06 AA08 BA05 BA07 BB03
BB10 CA06 CA08 CA09 CA14
CA16